



INFORMATION DISCLOSURE STATEMENT

1-6. U.S. Pat. Nos. 5,159,632, entitled "METHOD AND APPARATUS FOR PUBLIC KEY EXCHANGE IN A CRYPTOGRAPHIC SYSTEM"; 5,271,061, entitled "METHOD AND APPARATUS FOR PUBLIC KEY EXCHANGE IN A CRYPTOGRAPHIC SYSTEM"; 5,463,690, entitled "METHOD AND APPARATUS FOR PUBLIC KEY EXCHANGE IN A CRYPTOGRAPHIC SYSTEM"; 5,581,616, entitled "METHOD AND APPARATUS FOR DIGITAL SIGNATURE AUTHENTICATION"; 5,805,703, entitled "METHOD AND APPARATUS FOR DIGITAL SIGNATURE AUTHENTICATION"; and 6,049,610, entitled "METHOD AND APPARATUS FOR DIGITAL SIGNATURE AUTHENTICATION"; each disclose the use of a class of numbers in the form of $2^q - C$ which make modular reduction more efficient and, therefore, make cryptographic methods such as key exchange and digital signatures more efficient. The present invention does not use a class of numbers in the form of $2^q - C$.

7. The use of cryptographic key pairs was disclosed in U.S. Pat. No. 4,200,770, entitled "CRYPTOGRAPHIC APPARATUS AND METHOD." U.S. Pat. No. 4,200,770 also disclosed the application of key pairs to the problem of key agreement over an insecure communication channel. U.S. Pat. No. 4,200,770 does not disclose a method of cryptography based on elliptic curves as does the present invention.

8. Federal Information Processing Standards Publication 186-2 (i.e., FIPS PUB 186-2) discloses a digital signature standard. In the appendix of FIPS PUB 186-2 are recommended elliptic curves for a 192-bit, a 224-bit, a 256-bit, a 384-bit, and a 521-bit digital signature. The

elliptic curves disclosed in FIPS PUB 186-2 are different from the elliptic curves used in the present invention.

9-10. A book by N. Koblitz, "A Course in Number Theory and Cryptography," (1987), and a paper by V. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology - CRYPTO 85, LNCS 218, pp. 417-426, 1986, disclose the method of adapting discrete-logarithm based algorithms to the setting of elliptic curves. The elliptic curves disclosed in Koblitz and Miller are different from the elliptic curves used in the present invention.

11. A way to avoid explicit modular reduction is by carrying out arithmetic operations in the field F_p . This was first proposed by P. Montgomery in the paper "Modular multiplication without trial division," Mathematics of Computation, 44 (1985), pp. 519-521. This method has the advantage that it can be applied to both elliptic and non-elliptic cryptoalgorithms. However, Montgomery does not disclose the use of the elliptic curves of the present invention.

Please type a plus sign (+) inside this box →



PTO/SB/08B (08-00)

Approved for use through 10/31/2002. OMB 0651-0031

U. S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Complete if Known	
		Application Number	
		Filing Date	08-09-2001
		First Named Inventor	DR. JEROME A. SOLINAS
		Group Art Unit	
		Examiner Name	
Sheet 2 of 4	Attorney Docket Number	SOLINAS - 5	

OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS			
Examiner Initials [*]	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	1	FIPS PUB 186-2, 01-27-2000, DIGITAL SIGNATURE STANDARD, U.S. DEPT. OF COMMERCE (NIST)	
	2	VICTOR S. MILLER, "USE OF ELLIPTIC CURVES IN CRYPTOGRAPHY," ADVANCES IN CRYPTOGRAPHY - CRYPTO 85, LNCS 218, PP. 417-426, 1986	
	3	NEIL Koblitz, "A COURSE IN NUMBER THEORY AND CRYPTOGRAPHY," QA 241.K672, 1987, PP. 150-179.	
	4	PETER L. MONTGOMERY, "MODULAR MULTIPLICATION WITHOUT TRIAL DIVISION," MATHEMATICS OF COMPUTATION, VOL. 44, NO. 170, APRIL 1985, PP. 519-521	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.